Coherent eavesdropping strategies for the 4 state quantum cryptography protocol

J.I. Cirac[1,2] and N. Gisin[3]

(1) Departamento de Fisica Aplicada, Universidad de Castilla–La Mancha, 13071 Ciudad Real, Spain

(2) Institut für Theoretische Physik, Universität Innsbruck, A–6020 Innsbruck, Austria

(3) Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland

(February 1, 2008)

An elementary derivation of best eavesdropping strategies for the 4 state BB84 quantum cryptography protocol is presented, for both incoherent and two–qubit coherent attacks. While coherent attacks do not help Eve to obtain more information, they are more powerful to reveal the whole message sent by Alice. Our results are based on symmetric eavesdropping strategies, which we show to be sufficient to analyze these kind of problems.

PACS Nos. 03.65.Bz

In the 4-state BB84 quantum cryptography protocol [1], Alice, the *transmitter*, sends qubits in states chosen at random among a set of 4 possible states $\mathcal{S} = \{|0\rangle_z, |1\rangle_z, |0\rangle_x, |1\rangle_x\}$, where the subscripts z and x denote the polarization axis. At the other end of the quantum channel Bob, the *receiver*, analyzes the qubits in a basis chosen at random between $\{|0\rangle_z, |1\rangle_z\}$ (z basis) and $\{|0\rangle_x, |1\rangle_x\}$ (x basis). When Bob's basis happens to be compatible with the state sent by Alice, the only cases that the two partners will consider after publicly revealing the basis used for each qubit, Bob's results are perfectly correlated to the states sent by Alice. The safety of this protocol relies on the control of this perfect correlation and on the quantum principle that any eavesdropping necessarily perturbs the state of some of the qubits, hence reducing this correlation. Alice and Bob measure this correlation by publicly comparing a sample of their data. However, there is a practical question: given a measured correlation, how much information could have been collected by a malevolent third party, called traditionally Eve?

The general eavesdropping attack consists of first letting an auxiliary quantum system, called the probe, interact with the message (in form of qubits) sent by Alice [2]. Then, Eve waits until she knows the basis used in Bob's measurements, and extracts as much information as possible out of her probe. Thus, a given eavesdropping strategy can be characterized by a pair $(\mathcal{U}, \mathcal{M})$, where $\mathcal{U}$ is the unitary transformation used in the interaction between Eve's probe and the message, and $\mathcal{M}$ represents Eve's measurement. Most of the analysis of the best eavesdropping strategy so far have been concentrated in the so–called "incoherent attacks", in which each of Eve's probes interacts independently with each qubit sent by Alice. However, there might exist a better strategy for Eve in which her probes interact with more than one of Alice's qubits at the same time, what is known as "coherent attacks". This letter provides an elementary derivation of the optimal eavesdropping strategy for a given disturbance of the perfect correlation between Alice and Bob's data for both incoherent attacks and coherent attacks on two qubits. Our results show that coherent attacks do not help Eve to obtain more information about Alice message. However, they allow Eve to obtain the whole message sent by Alice with a higher probability. Thus, this is a situation where coherent attacks prove to be more powerful than incoherent (single qubit) ones [3] even if no error correction or privacy amplification [4] is performed.

Our formulation of the problem is based on what we will call "symmetric eavesdropping strategies". Those are attacks in which Eve treats all the possible messages sent by Alice on an equal footing. As we show below, without loss of generality, one can restrict oneself to analyze symmetric eavesdropping strategies only, which reduces enormously the problem. The reason is that for any given non–symmetric attack, coherent or incoherent, one can always find a symmetric one that reproduces the results of the non–symmetric strategy.

This paper is organized as follows: first, we consider general symmetric incoherent attacks; next, we consider general symmetric 2-qubit coherent attacks; and finally, we show that the symmetric strategies are sufficient to study eavesdropping attacks.

Let us analyze first the incoherent attacks. Denoting by $|E\rangle$ the initial state of Eve's probe, the unitary operation $\mathcal{U}$ can be characterized by its action on a basis set of Alice states

$$|E\rangle \otimes |0\rangle_z \xrightarrow{\mathcal{U}} |E^z_{0,0}\rangle|0\rangle_z + |E^z_{0,1}\rangle|1\rangle_z, \tag{1a}$$

$$|E\rangle \otimes |1\rangle_z \xrightarrow{\mathcal{U}} |E^z_{1,0}\rangle|0\rangle_z + |E^z_{1,1}\rangle|1\rangle_z, \tag{1b}$$

where $|E^z_{i,j}\rangle$ are unnormalized states of Eve's probe that span a 4–dimensional Hilbert space. Equation (1) can be written in a more compact form as

$$|E\rangle \otimes \begin{pmatrix} |0\rangle_z \\ |1\rangle_z \end{pmatrix} \xrightarrow{\mathcal{U}} \mathcal{E}^z \otimes \begin{pmatrix} |0\rangle_z \\ |1\rangle_z \end{pmatrix}, \tag{2}$$

where $\mathcal{E}^z$ is a 2×2 matrix whose elements are Eve's states $|E^z_{i,j}\rangle$. The action of $\mathcal{U}$ on the basis $\{|0\rangle_x, |1\rangle_x\}$ can be readily derived using linearity

$$|E\rangle \otimes \begin{pmatrix} |0\rangle_x \\ |1\rangle_x \end{pmatrix} \xrightarrow{\mathcal{U}} \mathcal{E}^x \otimes \begin{pmatrix} |0\rangle_x \\ |1\rangle_x \end{pmatrix}. \tag{3}$$

Here $\mathcal{E}^x = \mathcal{V}\mathcal{E}^z\mathcal{V}^\dagger$, where

$$\mathcal{V} = \mathcal{V}^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4}$$

implements the transformation from the z to the x basis.

Let us now particularize the above equations for a symmetric attack. To this aim, we note that for a given measurement strategy $\mathcal{M}$, the scalar products $\langle E^z_{i,j}|E^z_{k,l}\rangle$ characterize the unitary operation $\mathcal{U}$ of Eve's attack. In the present context, a symmetric attack is defined by imposing that all scalar products $\langle E^\alpha_{i,j}|E^\alpha_{k,l}\rangle$ ($\alpha = x, z$, $i, j, k, l = 0, 1$)) have to be invariant with respect to two operations: (i) exchange of the states $0 \leftrightarrow 1$; (ii) exchange of basis $z \leftrightarrow x$. This amounts to requiring that all possible states sent by Alice ($\in \mathcal{S}$) are treated on an equal footing. For example, the first condition (i) means that the probability amplitudes of any outcome should not depend on whether Alice prepared a $|0\rangle$ or a $|1\rangle$. It imposes that the scalar products should be invariant under the exchange of the subindices $0 \leftrightarrow 1$, i.e.,

$$F = \langle E_{0,0}|E_{0,0}\rangle = \langle E_{1,1}|E_{1,1}\rangle, \tag{5a}$$
$$D = \langle E_{0,1}|E_{0,1}\rangle = \langle E_{1,0}|E_{1,0}\rangle, \tag{5b}$$
$$F_1 = \langle E_{0,0}|E_{1,1}\rangle = \langle E_{1,1}|E_{0,0}\rangle, \tag{5c}$$
$$D_1 = \langle E_{0,1}|E_{1,0}\rangle = \langle E_{1,0}|E_{0,1}\rangle, \tag{5d}$$

etc, where traditionally F is called fidelity and D disturbance. The second condition (ii) means that the outcomes should not depend on whether Alice used the z or the x basis. Together with the normalization condition, it imposes that

$$F + D = 1, \qquad F - D = F_1 + D_1, \tag{6}$$

and that all the other scalar products that do not appear in (5) have to be zero. Thus, the number of independent parameters in the problem is reduced to only 2 real numbers (D and D_1, for example). Fixing the disturbance D, one can then determine any property of the attack (information gain, probability of success in guessing the qubit sent by Alice, etc) as a function of 1 parameter only. Therefore, best strategies can be very easily (even analytically) found by maximizing functions with respect to one parameter.

With these notations one can rewrite Eqs. (1) in the following appealing form:

$$|E\rangle \otimes |0\rangle_z \xrightarrow{\mathcal{U}} \sqrt{F}|\hat{E}^z_{0,0}\rangle|0\rangle_z + \sqrt{D}|\hat{E}^z_{0,1}\rangle|1\rangle_z \tag{7}$$

where $|\hat{E}^z_{j,k}\rangle$ represent Eve's (normalized) state in case Alice send a j bit and Bob detected a k bit. The fidelity F is the probability that Bob detected Alice bit correctly, while the disturbance D is the complementary probability of wrong detection.

Let us analyze now the measurement that allows Eve to extract the maximal information out of her probe. In principle, one should consider separately the cases in which Alice prepares each of the states $\mathcal{S}$, and then average over all these cases. However, thanks to the symmetry, it is sufficient to consider only the situation in which Alice chooses the z basis. In that case, after tracing over Alice's particle, Eve's two possible states are:

$$\rho_E(0) = |E^z_{0,0}\rangle\langle E^z_{0,0}| + |E^z_{0,1}\rangle\langle E^z_{0,1}|, \tag{8a}$$
$$\rho_E(1) = |E^z_{1,1}\rangle\langle E^z_{1,1}| + |E^z_{1,0}\rangle\langle E^z_{1,0}|, \tag{8b}$$

The optimal measurement strategy $\mathcal{M}$ for Eve is based on the fact that the four states that appear in the decomposition of these two density matrices, $|E^z_{i,j}\rangle$, fall into two mutually orthogonal sets, $S_0 = \{|E^z_{0,0}\rangle, |E^z_{1,1}\rangle\}$ and $S_1 = \{|E^z_{0,1}\rangle, |E^z_{1,0}\rangle\}$, that can be therefore distinguished deterministically. The first set S_0 occurs with probability F, in which case Eve has to extract information about two states with same a priori probability and overlap $\cos(\alpha) \equiv F_1/F$. The second set S_1 occurs with probability D and state overlap $\cos(\beta) \equiv D_1/D$ [5]. Consequently, Eve's information equals:

$$I_e = 1 + F\ H(P_\alpha) + D\ H(P_\beta), \tag{9}$$

where $H(P) = P\ln(P) + (1-P)\ln(1-P)$ is the Shanon entropy, and $P_\alpha = [1+\sin(\alpha)]/2$. The probability that Eve finds out the state sent by Alice is

$$P_e = F\ P_\alpha + D\ P_\beta. \tag{10}$$

These two quantities I_e and P_e are maximum for $\alpha = \beta$ (or, equivalently, $F_1/F = D_1/D$). In this case one has $D = [1-\cos(\alpha)]/2$, $I_e^{\rm opt} = 1 + H(P_\alpha)$, and $P_e^{\rm opt} = P_\alpha$. These relations provide the explicit and analytic optimum eavesdropping strategy with a single parameter α. It agrees with the numerical result and the bound devised in [6]. A complete presentation can be found in [7]. In Fig. 1 (upper plot) we have plotted $I_e^{\rm opt}$, Bob's information I_b, and $I_e^{\rm opt} + I_b$ as a function of D. In the lower plot we represent $P_e^{\rm opt}$ and Bob's probability $P_b = F$. For disturbances below 5%, as happens in experiments [8–10], the information gain is proportional to the disturbance: $I_e \approx 2\ln(2)D$. In this case a simpler 2–dimensional probe suffices [11]. On the other extreme, for $\alpha = \pi/3$ the disturbance is $\frac{1}{4}$ and the optimal information gain is 0.6454 (0.579 for 2-dimensional probe).

Let us conclude the analysis of incoherent attacks with the intriguing case when Bob's information $I_B = 1 + H(D)$ (probability of success $P_B = 1 - D$) equals Eve's optimum information $I_e^{\rm opt}$ ($P_e^{\rm opt}$). This occurs when $\cos(\alpha) = \sin(\alpha)$, i.e. when $\alpha = \pi/4$. Remarkably this coincides precisely with the threshold of violation of the Bell-CHSH inequality [12] by Alice and Bob. Indeed, the S parameter whose value is restricted below 2 by local realism, $S = 2\sqrt{2}\cos(\alpha) = 2$ for $\alpha = \pi/4$. This proves a conjecture presented in [11]. Another intriguing observation is that $I_e^{\rm opt} + I_b \leq 1$ (see Fig. 1); that is, the sum of the informations gained by Eve and Bob does not add to 1. This is due to the fact that Eve and Bob share an entangled state, and perform only local measurements.

Note however, that if Bob tells Eve the outcome of his measurement, then Eve can guess with certainty what was the qubit sent by Alice. In other words, if Bob and Eve are allowed to communicate one with each other, then, despite they do not perform joint measurements of the entangled state, they can determine the state sent by Alice.

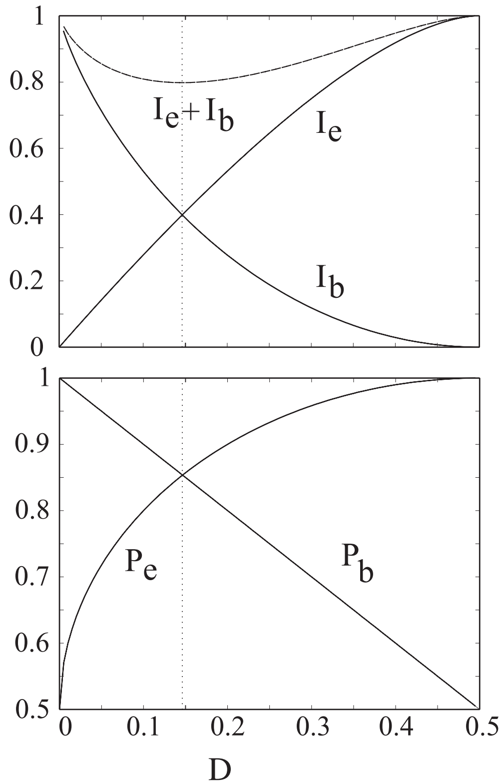

FIG. 1. Upper plot: Eve's optimum information $I_e^{\rm opt}$, Bob's information I_b, and $I_e^{\rm opt} + I_b$ (dashed line) as a function of the disturbance D. Lower plot: Eve's (P_e) and Bob's (P_b) probability of obtaining the message sent by Alice as a function of D.

We analyze now the possibility for Eve to interact coherently
with two qubits sent by Alice. We consider that Alice selects one of the 16 possible states among the set $\mathcal{S} = \{|0\rangle_z|0\rangle_z, |0\rangle_z|1\rangle_z, |1\rangle_z|0\rangle_z, |1\rangle_z|1\rangle_z, |0\rangle_x|0\rangle_z, |0\rangle_x|1\rangle_z, \ldots\}$. For convenience, we use binary notation: $|0\rangle_{zx} \equiv |0\rangle_z|0\rangle_x$, $|1\rangle_{xz} \equiv |1\rangle_x|0\rangle_z$, $|2\rangle_{zz} \equiv |0\rangle_z|1\rangle_z$, $|3\rangle_{xx} \equiv |1\rangle_x|1\rangle_x$, etc. Eve's unitary operation is characterized by the action of $\mathcal{U}$ on the basis zz

$$|E\rangle \otimes \begin{pmatrix} |0\rangle_{zz} \\ |1\rangle_{zz} \\ |2\rangle_{zz} \\ |3\rangle_{zz} \end{pmatrix} \xrightarrow{\mathcal{U}} \mathcal{E}^{zz} \otimes \begin{pmatrix} |0\rangle_{zz} \\ |1\rangle_{zz} \\ |2\rangle_{zz} \\ |3\rangle_{zz} \end{pmatrix}, \qquad (11)$$

where $\mathcal{E}$ is a 4×4 matrix containing Eve's probe states, i.e.,

$$\mathcal{U}|E\rangle \otimes |i\rangle_{zz} = \sum_{j=0}^{3} |E_{i,j}^{zz}\rangle \otimes |j\rangle_{zz}, \qquad (i = 0, \ldots, 3). \quad (12)$$

Taking into account the unitarity of $\mathcal{U}$, this operation is characterized by 240 real numbers (which are directly related to the scalar products of the elements of $\mathcal{E}^{zz}$). By imposing the conditions of a symmetric attack, and without loss of generality, the number of independent parameters is reduced to only 5.

The symmetric attack imposes now three conditions for the scalar products $\langle E_{i,j}^{zz}|E_{k,l}^{zz}\rangle$, which are analogous to the ones corresponding to the incoherent attack. They have to remain unchanged under: (i) the exchange $|0\rangle \leftrightarrow |1\rangle$ in the first qubit *or* the second qubit (independently); (ii) the exchange of the state of the first qubit by the state of the second qubit; (iii) the change of the basis (i.e., zz to xz or zx or xx). The first condition is equivalent to demanding that the scalar products have to remain unchanged if one exchanges all the subindices

$$1 \leftrightarrow 2 \qquad (13a)$$

The second condition implies invariance if one exchanges simultaneously the subindices

$$0 \leftrightarrow 1 \quad \text{and} \quad 2 \leftrightarrow 3. \qquad (13b)$$

Once this is satisfied, the third condition amounts to simply impose that $\langle E_{i,j}^{zz}|E_{k,l}^{zz}\rangle = \langle E_{i,j}^{xz}|E_{k,l}^{xz}\rangle, \forall i,j,k,l = 0,\ldots,3$, where the matrix $\mathcal{E}^{xz} = (\mathcal{V}\otimes 1)\mathcal{E}^{zz}(\mathcal{V}^\dagger \otimes 1)$, and $\mathcal{V}$ is defined in (4) [13]. In more detail, let us define the following parameters:

$$\begin{gathered} A = \langle E_{0,0}^{zz}|E_{0,0}^{zz}\rangle, \quad A_1 = \langle E_{0,0}^{zz}|E_{1,1}^{zz}\rangle, \quad A_2 = \langle E_{0,0}^{zz}|E_{3,3}^{zz}\rangle, \\ B = \langle E_{0,1}^{zz}|E_{0,1}^{zz}\rangle, \qquad B_1 = \langle E_{0,1}^{zz}|E_{1,0}^{zz}\rangle, \\ B_2 = \langle E_{0,1}^{zz}|E_{3,2}^{zz}\rangle, \qquad B_3 = \langle E_{0,1}^{zz}|E_{2,3}^{zz}\rangle, \\ C = \langle E_{0,3}^{zz}|E_{0,3}^{zz}\rangle, \quad C_1 = \langle E_{0,3}^{zz}|E_{1,2}^{zz}\rangle, \quad C_2 = \langle E_{0,3}^{zz}|E_{3,0}^{zz}\rangle. \end{gathered}$$

Imposing the symmetry and unitary conditions one finds that: *first*, the scalar product $\langle E_{i,j}^{zz}|E_{k,l}^{zz}\rangle$ is zero if among the indices (i,j,k,l) either three are identical and one is different or two are idential and two different [14]; *second*, each of the other scalar products are identical to one of these parameters [15]; *third*, all these parameters are real and fulfill the following relations [analogous to (6)]

$$\begin{aligned} A + 2B + C = 1, &\qquad B - C = B_3 + C_1, \\ A - B = A_1 + B_1, &\qquad A_1 - A_2 = B_2 + B_3, \\ B_1 - C_2 = B_2 + C_1 & \end{aligned} \qquad (14)$$

In this way, Eve's unitary transformation is fully characterized by only 5 real parameters.

By virtue of the symmetry, to determine Eve's disturbance we can consider the case in which Alice prepared the state $|0\rangle_{zz}$. One readily finds $D = 1 - (A + B)$. To determine Eve's gain of information, we can restrict ourselves to the case in which Alice used the zz basis to prepare the states. The density matrices that Eve obtains

for the 4 different choices of Alice qubits ($|0\rangle_{zz}, \ldots, |3\rangle_{zz}$) can be directly read off from the Eq. (12). Analogous to the incoherent attack case, Eve has first to distinguish among 4 orthogonal sets:

$$S_0 = \{|E^{zz}_{0,0}\rangle, |E^{zz}_{1,1}\rangle, |E^{zz}_{2,2}\rangle, |E^{zz}_{3,3}\rangle\}, \tag{15a}$$
$$S_1 = \{|E^{zz}_{0,1}\rangle, |E^{zz}_{1,0}\rangle, |E^{zz}_{2,3}\rangle, |E^{zz}_{3,2}\rangle\}, \tag{15b}$$
$$S_2 = \{|E^{zz}_{0,2}\rangle, |E^{zz}_{2,0}\rangle, |E^{zz}_{1,3}\rangle, |E^{zz}_{3,1}\rangle\}, \tag{15c}$$
$$S_3 = \{|E^{zz}_{0,3}\rangle, |E^{zz}_{3,0}\rangle, |E^{zz}_{1,2}\rangle, |E^{zz}_{2,1}\rangle\}, \tag{15d}$$

which occur with probabilities A, B, B, and C, respectively. This distinction can be performed with certainty, since the sets are mutually orthogonal. Then she has to find out which element of the corresponding set she has. To analyze that, note that in the case of S_0 and S_3, the four vectors form a pyramid with square base in a 4-dimensional Hilbert space [Fig. 2(a)], whereas in the case of S_1 and S_2, they form a pyramid with rectangular base [Fig. 2(b)]. For S_0 and S_3 there are two different overlaps among the four vectors, namely $\cos(\theta^0_{1,2}) = A_1/A, A_2/A$, and $\cos(\theta^3_{1,2}) = C_1/C, C_2/C$, respectively. For S_1 and S_2 there are three different overlaps $\cos(\theta^1_{1,2,3}) = \cos(\theta^2_{1,2,3}) = B_1/B, B_2/B, B_3/B$. Denoting by $\vec{a}^j_i$ $(i, j = 0, \ldots, 3)$ the i–th vector of the j–th set, we can then write the 4 vectors of any given set j in terms of an orthonormal (cartesian) basis $\vec{e}_0, \ldots, \vec{e}_3$ as

$$\begin{pmatrix} \vec{a}^j_0 \\ \vec{a}^j_1 \\ \vec{a}^j_2 \\ \vec{a}^j_3 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix} \begin{pmatrix} \vec{e}^j_0 \\ \vec{e}^j_1 \\ \vec{e}^j_2 \\ \vec{e}^j_3 \end{pmatrix}. \tag{16}$$

The coefficients satisfy the following equations:

$$a^2 + b^2 + c^2 + d^2 = 1, \qquad 2(ab + cd) = cos(\theta^j_1), \tag{17a}$$
$$2(ad + bc) = cos(\theta^j_2) \qquad 2(ac + bd) = cos(\theta^j_3), \tag{17b}$$

where we choose the solutions with $a > b, c, d$. Here, for the sake of compactness we have defined $\theta^{0,3}_3 = \theta^{0,3}_1$. We find that the best measurement corresponds to use the cartesian basis. For example, if the result is $\vec{e}_2$, then take as a guess the corresponding state $\vec{a}_2$.

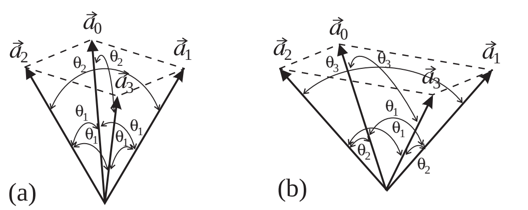

FIG. 2. Diagrammatic representation of the states of: (a) sets S_0 and S_3; (b) sets S_1 and S_2.

For a given set of 5 independent parameters using the relations (14) one first calculates the angles θ, as well as the probabilities of ending up with a given set S. Then one calculates the probabilities a^2, b^2, c^2 and d^2 for each given set by solving Eqs. (17). Starting from these probabilities, one can determine for a given disturbance D the probability for Eve to find out what was the message sent by Alice, as well as her information gain. We have found analytically that the strategy that gives Eve the maximum amount of information coincides with the incoherent attack analyzed above (Fig. 1). In contrast, the strategy that gives her maximum probability for determining the full message $(0, 1, 2,$ or $3)$ sent by Alice is different, and indeed relies on the use of a coherent attack.

If Fig. 3 we have plotted Eve's and Bob's probabilities P_e and P_b for guessing the two qubits sent by Alice as a function of the disturbance, both for the optimum incoherent attack P^1 as well as for the optimum coherent attack P^2 (this last, calculated numerically with a maximization procedure). In the lower insert we have plotted a detail of the curves around the disturbance which corresponds to violation of Bell's inequalities in the incoherent (single qubit) attack. In the upper insert we have plotted the relative gain of probability that Eve and Bob obtain using the coherent attack. This relative gain is rather small (smaller than 1.5%). For Eve it occurs at low disturbances, just where experiments take place.

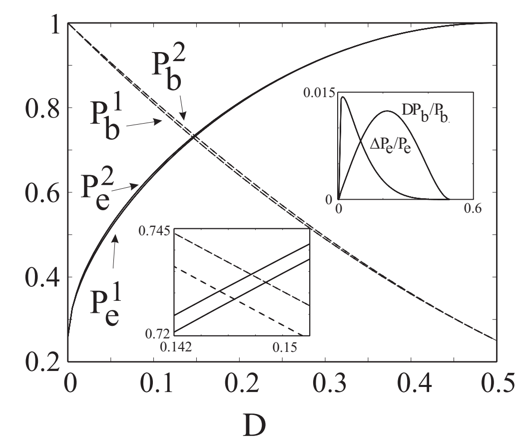

FIG. 3. Bob's (P_b) and Eve's (P_e) probabilities of guessing the two qubits sent by Alice for incoherent (P_1) and coherent (P_2) attacks. The inserts show a detail of the curves, as well as the relative gain of the coherent attack.

Let us notice that Bob could detect coherent attacks on successive pairs of qubit by controling the correlation of failures of successive qubits. However, Eve can prevent such a defense by attacking randomly chosen pairs of qubits, though at the cost of extra practical complications.

Let us conclude by sketching the proof that for a general case of coherent attack on n qubits $(n \geq 1)$, the analysis of what we have defined as symmetric strategies suffices. To do that we show that for any given strategy $\{\mathcal{U}, \mathcal{M}\}$ one can always construct a symmetric one $\{\mathcal{U}^s, \mathcal{M}^s\}$ that reproduces the results for all the prop-

erties which are defined as averages over the set $\mathcal{S}$ of possible states sent by Alice

$$\overline{Q} = \frac{1}{2^{2n}} \sum_{|\alpha\rangle \in \mathcal{S}} Q_\alpha. \tag{18}$$

For example if Q is the probability for Eve to guess the result sent by Alice, then Q_α would be this probability provided Alice has prepared the state $|\alpha\rangle$. Q could also be Eve's or Bob's information gain, the disturbance, etc.

The action of $\mathcal{U}$ is given, in general, by

$$\mathcal{U}|E\rangle \otimes |i\rangle_z = \sum_{j=0}^{2^n-1} |E_{i,j}\rangle \otimes |j\rangle_z, \qquad (i = 0, \ldots, 2^n - 1), \tag{19}$$

i.e., it is characterized by a matrix $\mathcal{E}$ with the states of Eve's probe [as in (11)]. Let us denote by $\mathcal{T}$ one of the operations (acting on Alice's qubits) that we have used to define the symmetric attack. To be more specific, we take $\mathcal{T}$ to be an operation that: (1) Is idempotent

$$\mathcal{T}^2 = 1; \tag{20a}$$

(2) Leaves Alice set of states invariant

$$\mathcal{T}\mathcal{S} = \mathcal{S}. \tag{20b}$$

For example,the operation corresponding to exchanging $0 \leftrightarrow 1$ in the q–th qubit (in the z basis) would be

$$\mathcal{T}|0\rangle_q = |1\rangle_q, \qquad \mathcal{T}|1\rangle_q = |0\rangle_q, \tag{21}$$

whereas the one corresponding to exchanging the basis $z \leftrightarrow x$ would be $\mathcal{T} \equiv \mathcal{V}$ defined in (4). Note that under these operations, $\mathcal{E}$ becomes $\mathcal{T}\mathcal{E}\mathcal{T}$.

We now construct explicitely a symmetric attack $\{\mathcal{U}^{\mathcal{T}}, \mathcal{M}^{\mathcal{T}}\}$ with respect to $\mathcal{T}$ [16]: (i) The action of $\mathcal{U}^{\mathcal{T}}$ is given by the matrix $\mathcal{E}^{\mathcal{T}} = \frac{1}{\sqrt{2}}(\mathcal{E}|0\rangle_e + \mathcal{T}\mathcal{E}\mathcal{T}|1\rangle_e)$, where $|0\rangle_e$ and $|1\rangle_e$ are two orthogonal states of an extra ancilla used by Eve and $\mathcal{E}|0\rangle_e$ is the matrix whose elements are the vectors obtained by applying the tensor product to the elements of $\mathcal{E}$ and the vector $|0\rangle_e$; (ii) Eve's measurement $\mathcal{M}^{\mathcal{T}}$ is defined as follows: first measure the state of the ancilla; if the result is $|0\rangle_e$, then use the original measurement strategy $\mathcal{M}$; if it is $|1\rangle_e$, then use the measurement strategy $\mathcal{M}$ that she would have applied if Alice state was prepared in the state $\mathcal{T}|\alpha\rangle$ instead of $|\alpha\rangle$. For example, for $\mathcal{T}$ corresponding to the change of basis $z \leftrightarrow x$, if Bob announces publically a measurement along the z axis and Eve obtains $|1\rangle_e$, then she should measure her probe as if Bob had announced a measurement in the x basis. Using (20a) one can readily check that $\{\mathcal{U}^{\mathcal{T}}, \mathcal{M}^{\mathcal{T}}\}$ fulfills $\langle \mathcal{E}^{\mathcal{T}}_{i,j} | \mathcal{E}^{\mathcal{T}}_{k,l} \rangle = \langle (\mathcal{T}\mathcal{E}^{\mathcal{T}}\mathcal{T})_{i,j} | (\mathcal{T}\mathcal{E}^{\mathcal{T}}\mathcal{T})_{k,l} \rangle$, i.e. it is symmetric with respect to $\mathcal{T}$. On the other hand, using (20b) one obtains that regardless of the result of the measurement on the ancilla, $\mathcal{M}^{\mathcal{T}}$ will give for Q the same result as the one given by the non–symmetric strategy (18). Using this procedure, one can then construct an attack $\{\mathcal{U}^s, \mathcal{M}^s\}$ that is symmetric with respect to all such operations $\mathcal{T}$, which it is what we have called a "symmetric eavesdropping strategy".

In conclusion, an analytic derivation of the incoherent eavesdropping strategy on the BB84 4 state quantum cryptography protocol that maximizes Eve's information has been presented. Using coherent attacks, i.e. assuming that Eve can interact coherently with more than one of the qubits send by Alice, seems not to improve Eve's information gain. This was proven for the 2-qubit case and we conjecture that this result hold for arbitrary coherent attacks. However, our analysis shows that coherent attacks can improve the probability that Eve guesses correctly the entire key, at the cost of higher probability that Eve guess is wrong on each qubit. This provides another example [3,?] that coherent (sometimes called collective) measurements can provide results unachievable with only incoherent measurements.

Helpful discussions with B. Huttner, N. Lutkenthaus, and P. Zoller are acknowledged. NG acknowledges financial support by the Swiss National Science Foundation. This work has been supported by the TMR newtork ERB–FMRX–CT96–0087.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038, 1996.

[3] C. Bennet, C. Fuchs, and J. Smolin, preprint (quant–ph/9611006).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Crypto **5**, 3, 1992.

[5] Note that at no additional cost (i.e., no additional disturbance), Eve knows whether Bob and Alice bits are identical (first set) or differ (second set). Therefore Eve's possesses the same information about the state prepared by Alice, as about the state received by Bob.

[6] Ch. Fuchs, A. Peres and R.B. Griffiths, private communications.

[7] C. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu and A. Peres, *Optimal eavesdropping in quantum cryptography*, submitted to Phys. Rev. A, 1997.

[8] P. D. Townsend, Electron. Letts. **30**, 809, 1993.

[9] A. Muller, H. Zbinden and N. Gisin, Nature **378**, 449, 1995.

[10] J. D.Franson and B. C. Jacobs, Electron. Letts. **31**, 232, 1995.

[11] N. Gisin and B. Huttner, "Quantum cloning, eavesdropping, and Bell's inequality" (preprint, quant-ph/9611041), Phys. Lett. A, in press, 1997.

[12] J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt,

Phys. Rev. Lett. **23**, 880, 1969.
[13] Due to the conditions (i) and (ii) one has actually to impose this only to a few elements.
[14] For example, $\langle E^{zz}_{0,2}|E^{zz}_{1,1}\rangle = \langle E^{zz}_{1,2}|E^{zz}_{1,3}\rangle = \langle E^{zz}_{0,2}|E^{zz}_{2,2}\rangle = 0$;
[15] For example, using (13a) one finds $B_1 = \langle E^{zz}_{0,1}|E^{zz}_{1,0}\rangle = \langle E^{zz}_{0,2}|E^{zz}_{2,0}\rangle$. Using (13b) one further finds $B_1 = \langle E^{zz}_{2,3}|E^{zz}_{3,2}\rangle = \langle E^{zz}_{1,3}|E^{zz}_{3,1}\rangle$.
[16] By symmetric attack with respect to a given operation $\mathcal{T}$ we mean that all the scalar products of the elements of $\mathcal{E}$ have to be invariant if one substitutes Alice state $|\alpha\rangle$ by $\mathcal{T}|\alpha\rangle$
[17] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).